

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-149103

(43)Date of publication of application : 02.06.1998

(51)Int.Cl.

G09C 1/00	G09C 1/00	G06F 15/00
G06F 17/60	G06F 19/00	G06K 17/00
G06K 19/10		

(21)Application number : 08-308063

(71)Applicant : MEYA TATSUHIRO

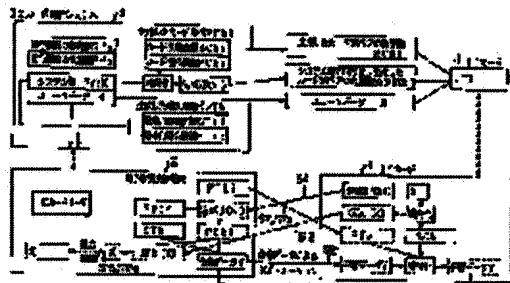
(22)Date of filing : 19.11.1996

(72)Inventor : MEYA TATSUHIRO

(54) METHOD AND SYSTEM FOR AUTHENTICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To eliminate the need for an on-line communication for user conformation between an electronic transaction/settlement terminal and a center device to detect an forged IC card by connecting to the center device by an off-line. **SOLUTION:** The IC card 1 has a secret key SCKi of generated pairs by card and is equipped with an open key Syek(PCki) of the generated pairs by cards, and unique data X is also set. The IC card receives an open key PTkj by terminals and arbitrary data from the electronic commerce terminal 2, generates SCKi (X) by chopherig from the unique data X and the secret key SCKi by cards, and supplies it to the terminal 2. The card 1 supplies Sysk(PCki) to the electric transaction/settlement terminal 2. The arbitrary data ciphered with the open key PTKj by terminals, secret key SCKi by cards, and arbitrary data is supplied to the terminal 2. The terminal 2 taken X out of SCKi (X) to perform matching and confirming operation.



対応なし、英抄

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-149103

(43)公開日 平成10年(1998)6月2日

(51) Int.Cl. ⁶	識別記号	F I
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00
	6 6 0	6 4 0 B
G 0 6 F 15/00	3 3 0	6 6 0 B
17/60		G 0 6 F 15/00
19/00		G 0 6 K 17/00
		G 0 6 F 15/21

審査請求 未請求 請求項の数 2 OL (全 14 頁) 最終頁に続く

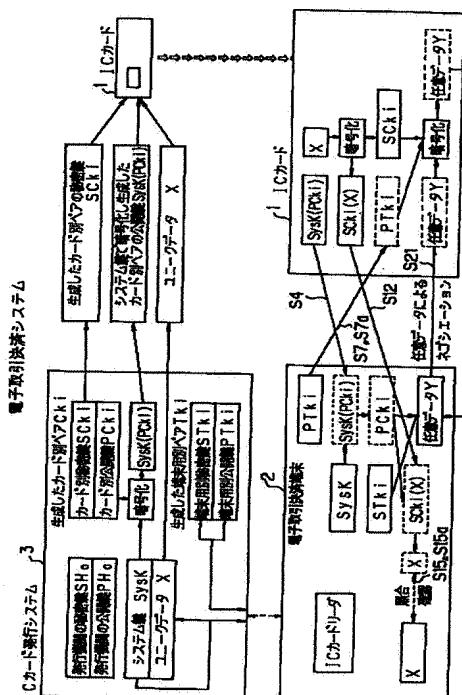
(21)出願番号	特願平8-308063	(71)出願人	595032185 女屋 達廣 東京都町田市原町田3-7-10 ハイコ ト矢口301
(22)出願日	平成8年(1996)11月19日	(72)発明者	女屋 達廣 東京都町田市原町田3-7-10 ハイコ ト矢口301
		(74)代理人	弁理士 萩野 平 (外5名)

(54)【発明の名称】 認証方法及び認証システム

(57)【要約】

【課題】 電子取引決済端末とセンタ装置との間でユーザ確認のためにオンライン通信する必要がなく、センタ装置とオフラインでICカードの偽造を検知すること。

【解決手段】 ICカード1には、生成したカード別ペアの秘密鍵SCKiが設定され、システム鍵で暗号化し生成したカード別ペアの公開鍵SySK (PCKi)が備えられ、ユニークデータXも設定されている。ICカード1は端末用別公開鍵PTkjと任意データとを電子取引決済端末2から受け取り、ユニークデータXとカード別秘密鍵SCKiとから暗号化してSCKi (X)を生成して端末2に与える。ICカード1はSySK (PCKi)を電子取引決済端末2に与える。端末用別公開鍵PTkjとカード別秘密鍵SCKiと任意データとから暗号化して暗号化任意データを端末2に与える。端末2は、SCKi (X)からXを取り出して、照合確認する。



【特許請求の範囲】

【請求項1】 カード1と端末2との間における認証方法において、

前記カード1に、カード別秘密鍵(SCKi)と、システム鍵で暗号化し生成したカード別公開鍵(SysK(PCKi))と、固有の情報であるユニークデータ(X)とを設定し、

前記端末2に、システム鍵(SysK)と、端末用別公開鍵(PTkj)と、端末用別秘密鍵(STkj)と、任意の情報である任意データ(Y)とを設定し、前記カード1と前記端末2との間で認証するために、

(1) 前記端末2の要求により、前記カード1に設定されている前記システム鍵で暗号化し生成したカード別公開鍵(SysK(PCKi))を前記端末2に出力し、

(2) 前記端末2で、前記システム鍵で暗号化し生成したカード別公開鍵(SysK(PCKi))を前記システム鍵(SysK)で復号して前記カード別公開鍵(PCKi)を取り出し、

(3) 前記端末用別公開鍵(PTkj)を前記カード別公開鍵(PCKi)で暗号化して前記カード1に出力し、

(4) 前記カード別秘密鍵(SCKi)で復号化して前記端末用別公開鍵(PTkj)を取り出し、

(5) 前記端末2の要求により、前記ユニークデータ(X)を生成し、

(6) 生成された前記ユニークデータ(X)を前記カード別秘密鍵(SCKi)で暗号化して前記端末2に出力し、

(7) 前記端末2で、前記カード別公開鍵(PCKi)で復号化して前記ユニークデータ(X)を取り出し、

(8) 前記端末2に設定されている前記端末用別秘密鍵(STkj)で前記ユニークデータ(X)を暗号化して前記カード1に出力し、かつ認証指示し、

(9) 前記カード1で、前記端末用別公開鍵(PTkj)で復号化して前記ユニークデータ(X)を取り出し、

(10) 前記カード1で、認証チェックし、認証チェックデータを前記端末2に出力し、

(11) 前記端末2で、前記認証チェックデータをチェックして第1次認証し、

(12) 前記端末2内で前記任意データ(Y)を生成し、

(13) 生成された任意データ(Y)を、(13-a) 前記端末用別秘密鍵(STkj)による暗号化(STkj(Y))、及び(13-b) 前記カード別公開鍵(PCKi)による暗号化(PCKi(Y))の何れか一方を前記カード1に出力し、

(14) 前記カード1で、(14-a) 前記端末用

別公開鍵(PTkj)による、前記(STkj(Y))及び(PCKi(Y))の何れか一方の復号化(Y又は?)、又は(14-b) 前記カード別秘密鍵(SCKi)による、前記(STkj(Y))及び前記(PCKi(Y))の何れか一方の復号化(?)又はYによりデータ(Y,?)を取り出し、

(15) 前記カード1で、(15-a) 前記カード別秘密鍵(SCKi)による前記(14-a)の出力(Y)の暗号化(SCKi(Y))及び前記端末用別公開鍵(PTkj)による前記(14-a)の出力(?)の暗号化(PTkj(?))、又は(15-b) 前記カード別秘密鍵(SCKi)による前記(14a)の出力(?)の暗号化(SCKi(?))及び前記端末用別公開鍵(PTkj)による前記(14-a)の出力(Y)の暗号化(PTkj(Y))を前記端末2に出力し、

(16) 前記端末2で、(16-a) 前記カード別公開鍵(PCKi)による前記(15-a)の出力(SCKi(Y))の復号化(Y)及び前記端末用別秘密鍵(STkj)による前記(15-a)の出力(PTkj(?))の復号化(?)、又は(16-b) 前記カード別公開鍵(PCKi)による前記(15-b)の出力(SCKi(?))の復号化(?)及び前記端末用別秘密鍵(STkj)による前記(15-b)の出力(PTkj(Y))の復号化(Y)によりデータペア(Y,?)を取り出し、

(17) 前記端末2で、前記(16)で得られたデータペア(Y,?)が正しいか否かを判断して第2次認証することを特徴とする認証方法。

【請求項2】 カード発行システム3と、カード1と、端末2とを備えた認証システムにおいて、前記カード発行システム3には、発行機関の秘密鍵(SH。)及び発行機関の公開鍵(PH。)と、生成したカード別ペア鍵(Cki)を構成するカード別秘密鍵(SCKi)及びカード別公開鍵(PCKi)と、システム鍵(SysK)と、固有の情報であるユニークデータ(X)と、生成した端末用別ペア鍵(Tkj)を構成する端末用別秘密鍵(STkj)及び端末用別公開鍵(PTkj)とが設定され、

前記カード1には、前記カード別秘密鍵(SCKi)と、システム鍵で暗号化し生成したカード別公開鍵(SysK(PCKi))と、前記ユニークデータ(X)とが設定され、

前記端末2には、前記システム鍵(SysK)と、前記端末用別公開鍵(PTkj)と、前記端末用別秘密鍵(STkj)と、任意の情報である任意データ(Y)と、前記カード1に設定された内容を読取るカードリーダとが設定されており、

前記カード1と前記端末2との間で認証するために、前記カード1が前記端末2の前記カードリーダに装着され

ると、

(1) 前記端末2の要求により、前記カード1に設定されている前記システム鍵で暗号化し生成したカード別公開鍵($SysK(PCki)$)が前記端末2に出力され、

(2) 前記端末2で、前記システム鍵で暗号化し生成したカード別公開鍵($SysK(PCki)$)が前記システム鍵($SysK$)で復号されて、前記カード別公開鍵($PCki$)が取り出され、

(3) 前記端末用別公開鍵($PTkj$)が前記カード別公開鍵($PCki$)で暗号化されて前記カード1に出力され、

(4) 前記カード別秘密鍵($SCki$)で復号化されて前記端末用別公開鍵($PTkj$)が取り出され、

(5) 前記端末2の要求により、前記ユニークデータ(X)が生成され、

(6) 生成された前記ユニークデータ(X)が前記カード別秘密鍵($SCki$)で暗号化されて前記端末2に出力され、

(7) 前記端末2で、前記カード別公開鍵($PCki$)で復号化されて前記ユニークデータ(X)が取り出され、

(8) 前記端末2に設定されている前記端末用別秘密鍵($STkj$)で前記ユニークデータ(X)が暗号化されて前記カード1に出力され、かつ認証指示され、

(9) 前記カード1で、前記端末用別公開鍵($PTkj$)で復号化されて前記ユニークデータ(X)が取り出され、

(10) 前記カード1で、認証チェックされ、認証チェックデータが前記端末2に出力され、

(11) 前記端末2で、前記認証チェックデータをチェックすることにより第1次認証され、

(12) 前記端末側2で、前記任意データ(Y)が生成され、

(13) 生成された前記任意データ(Y)が、(13-a) 前記端末用別秘密鍵($STkj$)による暗号化($STkj(Y)$)、及び(13-b) 前記カード別公開鍵($PCki$)による暗号化($PCki(Y)$)の何れか一方が前記カード1に出力され、

(14) 前記カードで、(14-a) 前記端末用別公開鍵($PTkj$)による、前記($STkj(Y)$)及び($PCki(Y)$)の何れか一方の復号化(Y 又は $?$)、又は(14-b) 前記カード別秘密鍵($SCki$)による、前記($STkj(Y)$)及び前記($PCki(Y)$)の何れか一方の復号化($?$ 又は Y)によりデータ(Y 、 $?$)が取り出され、

(15) 前記カード1で、(15-a) 前記カード別秘密鍵($SCki$)による前記(14-a)の出力(Y)の暗号化($SCki(Y)$)及び前記端末用別公開鍵($PTkj$)による前記(14-a)の出力($?$)

10

の暗号化($PTkj(?)$)、又は(15-b) 前記カード別秘密鍵($SCki$)による前記(14-a)の出力($?$)の暗号化($SCki(?)$)及び前記端末用別公開鍵($PTkj$)による前記(14-a)の出力(Y)の暗号化($PTkj(Y)$)が前記端末2に出力され、

(16) 前記端末2で、(16-a) 前記カード別公開鍵($PCki$)による前記(15-a)の出力($SCki(Y)$)の復号化(Y)及び前記端末用別秘密鍵($STkj$)による前記(15-a)の出力($PTkj(?)$)の復号化($?$)、又は(16-b) 前記カード別公開鍵($PCki$)による前記(15-b)の出力($SCki(?)$)の復号化($?$)及び前記端末用別秘密鍵($STkj$)による前記(15-b)の出力($PTkj(Y)$)の復号化(Y)によりデータペア(Y 、 $?$)が取り出され、

(17) 前記端末2で、前記(16)で得られたデータペア(Y 、 $?$)が正しいか否かを判断することにより第2次認証されることを特徴とする認証システム。

20

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証方法及び認証システムに係わり、特に、電子現金金融システムなどに適用し得る電子取引決済での認証に関する。

【0002】

【従来の技術】近年、ICカードと電子取引決済端末とセンタ装置を使用した金融商品の取引のための電子取引決済システム(例えば、クレジット決済システム)及びそのシステムにおける電子取引決済方法又は認証方法が開発されている。従来の電子取引決済システムにおいて、ICカードは、個々のユーザに秘密鍵を割り当て、個人情報などと共にICカードに設定し、ICカード発行機関からオフラインで発行される。この秘密鍵は、秘密鍵暗号方式(共通鍵暗号方式、例えば、DES)又はRSAによる公開鍵暗号方式(非対象暗号系)によって暗号化されている。

30

【0003】電子取引決済時に、電子取引決済端末のカードリーダにICカードが装着される。カードリーダは、ICカードの内容に対して暗号解読(復号化)して設定情報を読み取り、個々を認証するために、センタ装置とオンライン通信する。この認証が正しくできれば、電子取引決済する。

40

【0004】

【発明が解決しようとする課題】しかしながら、従来の電子取引決済システムでは、電子取引決済端末と、センタ装置との間でオンライン通信によってユーザのICカードのユーザ情報が正しいか否かを確認する必要がある。ところが、公開鍵暗号方式(RSA)を使用しても、オフラインの場合は、本人以外の第3者によるICカード偽造を検知することができない。

50

【0005】また、システム的な鍵を使用していても、万一そのシステム的鍵が漏洩された場合に、全システムの危機となる。

【0006】このようなことから、電子取引決済端末とセンタ装置（又はホスト装置）との間でユーザ確認のためにオンライン通信する必要がなく、オフラインで電子取引決済端末がICカードの偽造を検知でき、システム的な鍵が漏洩されても全体システムの危機とならない電子取引決済システム及び認証方法の実現が要請されている。

【0007】

【課題を解決するための手段】そこで、本発明に係わる認証方法は、カード1と端末2との間における認証方法において、以下の構成で上述の課題を解決する。すなわち、前記カード1に、カード別秘密鍵（SCKi）と、システム鍵で暗号化し生成したカード別公開鍵（SysK（PCKi））と、固有の情報であるユニークデータ（X）とを設定し、前記端末2に、システム鍵（SysK）と、端末用別公開鍵（PTkj）と、端末用別秘密鍵（STkj）と、任意の情報である任意データ（Y）とを設定し、前記カード1と前記端末2との間で認証するため、

(1) 前記端末2の要求により、前記カード1に設定されている前記システム鍵で暗号化し生成したカード別公開鍵（SysK（PCKi））を前記端末2に出力し、

(2) 前記端末2で、前記システム鍵で暗号化し生成したカード別公開鍵（SysK（PCKi））を前記システム鍵（SysK）で復号して前記カード別公開鍵（PCKi）を取り出し、

(3) 前記端末用別公開鍵（PTkj）を前記カード別公開鍵（PCKi）で暗号化して前記カード1に出力し、

(4) 前記カード別秘密鍵（SCKi）で復号化して前記端末用別公開鍵（PTkj）を取り出し、

(5) 前記端末2の要求により、前記ユニークデータ（X）を生成し、

(6) 生成された前記ユニークデータ（X）を前記カード別秘密鍵（SCKi）で暗号化して前記端末2に出力し、

(7) 前記端末2で、前記カード別公開鍵（PCKi）で復号化して前記ユニークデータ（X）を取り出し、

(8) 前記端末2に設定されている前記端末用別秘密鍵（STkj）で前記ユニークデータ（X）を暗号化して前記カード1に出力し、かつ認証指示し、

(9) 前記カード1で、前記端末用別公開鍵（PTkj）で復号化して前記ユニークデータ（X）を取り出し、

(10) 前記カード1で、認証チェックし、認証チ

ックデータを前記端末2に出力し、

(11) 前記端末2で、前記認証チェックデータをチェックすることにより第1次認証し、

(12) 前記端末2内で前記任意データ（Y）を生成し、

(13) 生成された任意データ（Y）を、(13-a) 前記端末用別秘密鍵（STkj）による暗号化

(STkj(Y)、及び(13-b) 前記カード別公開鍵（PCKi）による暗号化（PCKi(Y)）の何れか一方を前記カード1に出力し、

(14) 前記カード1で、(14-a) 前記端末用別公開鍵（PTkj）による、前記（STkj(Y)）及び（PCKi(Y)）の何れか一方の復号化（Y又は?）、又は(14-b) 前記カード別秘密鍵（SCKi）による、前記（STkj(Y)）及び前記（PCKi(Y)）の何れか一方の復号化（?又はY）によりデータ（Y、?）を取り出し、

(15) 前記カード1で、(15-a) 前記カード別秘密鍵（SCKi）による前記（14-a）の出力

20 (Y)の暗号化（SCKi(Y)）及び前記端末用別公開鍵（PTkj）による前記（14-a）の出力（?）の暗号化（PTkj（?））、又は(15-b) 前記カード別秘密鍵（SCKi）による前記（14-a）の出力（?）の暗号化（SCKi（?））及び前記端末用別公開鍵（PTkj）による前記（14-a）の出力（Y）の暗号化（PTkj(Y)）を前記端末2に出力し、

(16) 前記端末2で、(16-a) 前記カード別公開鍵（PCKi）による前記（15-a）の出力（S

30 Cki(Y)）の復号化（Y）及び前記端末用別秘密鍵（STkj）による前記（15-a）の出力（PTkj（?））の復号化（?）、又は(16-b) 前記カード別公開鍵（PCKi）による前記（15-b）の出力（SCKi（?））の復号化（?）及び前記端末用別秘密鍵（STkj）による前記（15-b）の出力（PTkj(Y)）の復号化（Y）によりデータペア（Y、?）を取り出し、

(17) 前記端末2で、前記（16）で得られたデータペア（Y、?）が正しいか否かを判断することにより第2次認証する。

【0008】また、本発明に係わり認証システムは、カード発行システム3と、カード1と、端末2とを備えた認証システムにおいて、以下の構成で上述の課題を解決する。すなわち、前記カード発行システム3には、発行機関の秘密鍵（SH。）及び発行機関の公開鍵（PH。）と、生成したカード別ペア鍵（CKi）を構成するカード別秘密鍵（SCKi）及びカード別公開鍵（PCKi）と、システム鍵（SysK）と、固有の情報であるユニークデータ（X）と、生成した端末用別ペア鍵（Tkj）を構成する端末用別秘密鍵（STkj）及び

7
端末用別公開鍵 (PTkj) とが設定され、前記カード1には、前記カード別秘密鍵 (SCKi) と、システム鍵で暗号化し生成したカード別公開鍵 (SysK (PCki)) と、前記ユニークデータ (X) とが設定され、前記端末2には、前記システム鍵 (SysK) と、前記端末用別公開鍵 (PTkj) と、前記端末用別秘密鍵 (STkj) と、任意の情報である任意データ (Y) と、前記カード1に設定された内容を読取るカードリーダとが設定されており、前記カード1と前記端末2との間で認証するために、前記カード1が前記端末2の前記カードリーダに装着されると、

(1) 前記端末2の要求により、前記カード1に設定されている前記システム鍵で暗号化し生成したカード別公開鍵 (SysK (PCki)) が前記端末2に出力され、

(2) 前記端末2で、前記システム鍵で暗号化し生成したカード別公開鍵 (SysK (PCki)) が前記システム鍵 (SysK) で復号されて、前記カード別公開鍵 (PCki) が取り出され、

(3) 前記端末用別公開鍵 (PTkj) が前記カード別公開鍵 (PCki) で暗号化されて前記カード1に出力され、

(4) 前記カード別秘密鍵 (SCKi) で復号化されて前記端末用別公開鍵 (PTkj) が取り出され、

(5) 前記端末2の要求により、前記ユニークデータ (X) が生成され、

(6) 生成された前記ユニークデータ (X) が前記カード別秘密鍵 (SCKi) で暗号化されて前記端末2に出力され、

(7) 前記端末2で、前記カード別公開鍵 (PCki) で復号化されて前記ユニークデータ (X) が取り出され、

(8) 前記端末2に設定されている前記端末用別秘密鍵 (STkj) で前記ユニークデータ (X) が暗号化されて前記カード1に出力され、かつ認証指示され、

(9) 前記カード1で、前記端末用別公開鍵 (PTkj) で復号化されて前記ユニークデータ (X) が取り出され、

(10) 前記カード1で、認証チェックされ、認証チェックデータが前記端末2に出力され、

(11) 前記端末2で、前記認証チェックデータがチェックされて第1次認証され、

(12) 前記端末側2で、前記任意データ (Y) が生成され、

(13) 生成された前記任意データ (Y) が、(13-a) 前記端末用別秘密鍵 (STkj) による暗号化 (STkj (Y))、及び (13-b) 前記カード別公開鍵 (PCki) による暗号化 (PCki (Y)) の何れか一方が前記カード1に出力され、

(14) 前記カードで、(14-a) 前記端末用別

公開鍵 (PTkj) による、前記 (STkj (Y)) 及び (PCki (Y)) の何れか一方の復号化 (Y又は?)、又は (14-b) 前記カード別秘密鍵 (SCKi) による、前記 (STkj (Y)) 及び前記 (PCki (Y)) の何れか一方の復号化 (?)又はY)によりデータ (Y, ?) が取り出され、

(15) 前記カード1で、(15-a) 前記カード別秘密鍵 (SCKi) による前記 (14-a) の出力 (Y) の暗号化 (SCKi (Y)) 及び前記端末用別公開鍵 (PTkj) による前記 (14-a) の出力 (?) の暗号化 (PTkj (?))、又は (15-b) 前記カード別秘密鍵 (SCKi) による前記 (14-a) の出力 (?) の暗号化 (SCKi (?)) 及び前記端末用別公開鍵 (PTkj) による前記 (14-a) の出力 (Y) の暗号化 (PTkj (Y)) が前記端末2に出力され、

(16) 前記端末2で、(16-a) 前記カード別公開鍵 (PCki) による前記 (15-a) の出力 (SCKi (Y)) の復号化 (Y) 及び前記端末用別秘密鍵 (STkj) による前記 (15-a) の出力 (PTkj (?)) の復号化 (?)、又は (16-b) 前記カード別公開鍵 (PCki) による前記 (15-b) の出力 (SCKi (?)) の復号化 (?) 及び前記端末用別秘密鍵 (STkj) による前記 (15-b) の出力 (PTkj (Y)) の復号化 (Y) によりデータペア (Y, ?) が取り出され、

(17) 前記端末2で、前記 (16) で得られたデータペア (Y, ?) が正しいか否かを判断することにより第2次認証する。

30 【0009】このような構成をとることで、端末とカードとはオフラインであり、システム鍵が端末にのみあり、カードの公開鍵は端末でのみ取り出すことができる。仮に、偽造などによって第1次認証を通過しても、公開鍵と秘密鍵とのペアを取得してネゴシエーションすることができないため、第2次認証を通過することはできない。

【0010】

【発明の実施の形態】次に本発明の好適な実施の形態を図面を用いて説明する。本実施の形態の電子取引決済システムは、従来のセンタ装置と電子取引決済端末との間でオンライン通信によってユーザカード認証のために確認しなくとも、ユーザICカードと電子取引決済端末との間で確認することにより安全に認証及び電子取引決済することができるよう構成される。

【0011】即ち、ユーザICカードに、公開鍵と秘密鍵とのデータペアが存在しないようにする。システム鍵が電子取引決済端末にだけあり、ユーザICカードの公開鍵は電子取引決済端末側でだけ取り出せるようにする。電子取引決済端末での第1次認証用データを外部より特定できないようにする。第1次認証用データが電子

取引決済端末にだけあり、ユーザICカードから取り出した公開鍵でのみ認証可能とする。

【0012】仮に、第1次認証用データを万一正常に通過（クリア）したとしても、電子取引決済端末での任意データを認証確認用データに加工するための、公開鍵と秘密鍵とのペアを取得してネゴシエーションができないようにして、第2次認証を通過できないように構成される。また、第3者による偽造ICカードが勝手に公開鍵及び秘密鍵のペアを作り出した場合でも、システム鍵を知らないため、電子取引決済端末側が解読できる公開鍵を有するシステム鍵を作り出せないため、ネゴシエーションエラーによって偽造ICカードであることを検知するように構成される。

【0013】図1は、電子取引決済システムの構成図である。この図1において、電子取引決済システムは、ICカード1と、電子取引決済端末2と、ICカード発行システム3とから構成されている。ICカード発行システム3は、ICカード製造固有情報書き込み機能を有し、ICカード内蔵ROMソフト書き込み機能を有し、発行済のチェック機能を有し、ICカード初期化情報書き込み機能として、例えば、ICカードID（識別）固有情報と公開鍵（暗号化鍵と復号化鍵とを生成）とを有し、利用者固有情報書き込み（例えば、氏名、住所、性別、年令、パスワード等）機能を有し、ICカード発行機能を有し、発行監査情報作成機能を有し、発行情報通信機能などを有する。

【0014】ICカード発行システム3は、具体的には、発行機関の秘密鍵SH_i及び発行機関の公開鍵PH_iを備え、カード別秘密鍵SCK_i及びカード別公開鍵PCK_iを生成し、システム鍵SysKを備え、このシステム鍵SysKに対してカード別秘密鍵SCK_i及びカード別公開鍵PCK_iによって暗号化し、SysK(PCK_i)を得る。更に、ICカード発行機関3は、ユニークデータXを備え、端末用別秘密鍵STK_j及び端末用別PTK_jを備える。

【0015】ICカード発行システム3は、生成したICカード別ペアの秘密鍵SCK_iと、システム鍵で暗号化し生成したカード別ペアの公開鍵SysK(PCK_i)と、ユニークデータXとをICカード1に書き込む。

【0016】(ICカード1の内部機能) ICカード1は、オンライン時、オフライン時の認証情報出力機能を備え、ICカード1の格納金額表示機能を備え、アプリケーション情報の入出力管理機能を備える。このアプリケーション情報の入出力管理機能は、具体的には、アプリケーション別の権限識別鍵情報の管理、情報の蓄積/出力、監査情報の作成、パスワードチェック又はロックなどである。

【0017】(電子取引決済端末2の機能) 電子取引決済端末2は、ICカード1を認証する機能（例えば、ネ

ゴシエーション情報の確認、認証確認機能）を備え、ユーザ操作機能（例えば、各種操作入力、チェック、チェック用情報作成機能）を備え、オンライン時及びオフライン時の情報通信機能を備え、情報格納管理機能（例えば、端末側情報作成機能、監査情報作成機能）を備え、鍵情報管理機能を備える。

【0018】(認証確認シーケンス) ICカードの製造発行時、ICカードの固体固有情報は、ロックオフエリアに書き込まれる。ロックオフエリアは、内蔵ROMのプログラムでもアクセス可能である。ICカード確認用固定鍵は、システム鍵+ロックオフ鍵形態で二重暗号化され、ロックアップエリアへセットされる。

【0019】ユーザ固有情報は、システム鍵+パスワード+ロックオフ鍵形態で三重暗号化されて、システムエリアへセットされる。公開鍵方式のペアの鍵がシステムエリアへセットされる。即ち、暗号化鍵は、システム鍵+ロックオフ鍵形態で二重暗号化される。復号化鍵は、ロックオフ鍵で暗号化される。ICカード使用時は、カード本体をチェックする。具体的には、ロックアップエリアをそのまま読み取り、ICカード確認用固定鍵をシステム鍵で暗号化したものとの不一致を確認する。内蔵ROMのシステムをチェックサムして、変更されていないかを確認する。任意に端末側で作成したデータをシステム鍵で暗号化したものと、ICカードに渡す。

【0020】ICカード側ではロックアップエリアの情報をロックオフ鍵で復号化してICカード確認用鍵を取り出し、この鍵で端末から受け取った情報を暗号化して端末に返す。端末側では、ICカードに渡したデータを事前にICカード確認用鍵で暗号化しておき、端末から返ったデータと一致するか否かを確認する。認証確認後、オフライン時は公開鍵を交換する（ICカードと端末間）。ここでも、万一偽造カードの場合、勝手に公開鍵ペアを作ったとしても、システム鍵が分からなければ、端末側に渡すべきICカードの公開鍵をシステム鍵で暗号化したデータを作れない。その結果、端末との通信ができなくなる。

【0021】認証確認後、オフライン時では、セキュリティの実体は全て端末側のコントロールとなり、端末側の情報のセキュリティ度合いによる。端末は、ICカードより一層厳重なチップの中に、固有情報が埋め込まれ、例えば、端末ごと盗み出されても鍵情報を取り出すことはできない。

【0022】(ICカード1の固有情報の作成) ロックオフ又はロックノンへ固有情報が書き込まれる。ICカードへ内蔵ロジックが書き込まれる。認証確認情報（認証する際の通信情報を暗号化する鍵）が書き込まれる。但し、固有情報によって暗号化されることで、全てのICカードごとに異なった情報になり、外部からは鍵の解読ができない。

【0023】ICカード別通信用の公開鍵・秘密鍵を生

成し、書き込む。秘密鍵はそのまま保存されるので、端末への通信情報を暗号化できる。但し、公開鍵は、システム鍵によって暗号化され、ICカードに保存され、端末と通信する際にそのデータが端末に送付される。端末では、システム鍵によってICカードの公開鍵を取り出し、ICカードとの通信時に使用される。

【0024】電子取引決済端末2は、端末の秘密鍵、公開鍵及びシステム鍵を格納する。電子取引決済端末2は、端末の公開鍵を送付し、システム鍵（ICカードの公開鍵）を受け取り、ICカード1の公開鍵を取り出す。電子取引決済端末2の通信時に使用する情報は、端末の秘密鍵及びICカードの公開鍵である。ICカード1は、カードの秘密鍵を格納し、システム鍵（ICカードの公開鍵）を格納する。ICカード1は、システム鍵を送付し、端末の公開鍵を受け取る。ICカード1の通信時使用する情報は、ICカードの秘密鍵と端末の公開鍵とである。

【0025】（偽造カードの真偽チェック）認証確認情報がカード固有情報になっているか否かを確認する（チェックポイント情報の確認）。尚、この情報は、内蔵ロジックが利用する鍵情報となっている。内蔵ロジックのチェックサム情報等を確認する（ロジック改ざん防止）。端末側からの任意データをICカードに渡し、暗号化処理し、改ざん又は偽造されたカードを確認する（カード偽造防止）。カード内の個人情報は全てパスワードで二重に暗号化されているので、入力された変数としてのパスワードで復号化して、意味のあるデータの取り出しができるか否かで、該当カード情報の認証を確認する。

【0026】ICカード別固有の秘密鍵・公開鍵ペアの情報を土台として、最終確認情報（ネゴシエーション）を交換して、正式ユーザとして認定される（カード偽造・認証確認）。

【0027】（認証シーケンスの概要）図2、図3は、認証シーケンスの概要である。端末側からのデータ保全に関しては、全て端末の鍵管理システムと端末用CPUによって端末に格納されている各種鍵情報が保全されていることが前提である。先ず、初期情報設定として、ICカードの固体固有情報を書き込む。端末側で製造No.21及びシステムロジック23をICカード側に与え、製造No.22はロックオフェリアに書き込み、システムロジック24は内蔵ROMに書き込む。

【0028】カード発行時、端末側は認証確認情報26をICカード側に与え、製造No.25を用いて暗号化27して認証確認情報28としてロックアップエリアに書き込む。この認証確認情報28は、端末側に与えられ、カード真偽が確認される。具体的には、初期情報設定として、内蔵ロジックチェックのため、先ず、ロックアップエリアを読み取り、不一致確認のための比較29を実行し、認証確認情報30を得る。

【0029】次に、第1次内蔵ロジックの確認のため、ICカード側は、システムロジック31からチェックサム32を計算し、このチェックサム結果33を端末側に与え、一致確認のための比較34を実行し、チェックサム結果35を出力する。次に、内蔵セキュリティロジックと外部固有エリアの対応によってカード本体の偽造をチェックするために、ICカード側で、認証確認用情報36と、製造No.37とから復号化38を実行し、認証確認用情報39を得て、端末側からの任意データ40を認証確認用情報39で暗号化41し、暗号化された任意データ42を端末側に与える。

【0030】次に、端末側では任意データ43とシステム鍵44とから暗号化45して暗号化した任意データ46を得る。この任意データ46は、ICカード側に与えると共に認証確認用情報47と暗号化48して暗号化された任意データ50を得て、ICカード側からの任意データ42と一致確認するために比較49を実行する。この処理によって、本体の本物の確認を完了する。

【0031】次に、個人情報の定型の情報がパスワードで暗号化されているので、システムエリアの個人情報を読み取るため、ICカード側からシステムエリアの個人情報51と、ロックオフェリアの製造No.とから復号化53し、得られる個人情報54を端末側に与える。端末側では、個人情報55と、入力パスワード56とから復号化57を実行し、個人情報58を得る。この個人情報58とシステム鍵59とから復号化60を実行し、個人情報61を得る。これによって、意味ある情報の入手を確認することによって認証が確認される（認証確認終了）。

【0032】次に、公開鍵を交換処理するために、先ず、端末からの送付として、公開鍵（暗号鍵）62をICカード側に送信する。次に、ICカード側から公開鍵64を端末側に与える。端末側では公開鍵65とシステム鍵66とから復号化67を実行し、公開鍵68を得る。ICカード側には、システム鍵がないので偽造することができない。

【0033】（ICカード1と電子取引決済端末2との相互認証の処理動作）次に、図1の構成において、ICカード1の相互認証の処理動作を図4、図5を用いて説明する。

【0034】先ず、図4において、ICカード1を電子取引決済端末2のカードリーダに挿入する（ステップS1）。これによって電子取引決済端末2は、ICカード1に対してICカード1の公開鍵出力を要求する（ステップS2）。これによって、ICカード1は、公開鍵を出力し（ステップS4）、カード別公開鍵を端末システム用システム鍵で暗号化したSYSK（PCKi）を電子取引決済端末2に与える（ステップS5）。

【0035】ICカード1の公開鍵を取り出して（ステップS6）、端末システム用システム鍵SYSKで復号

化する（ステップS6a）。次に、ICカード1のカード別公開鍵PCKiで電子取引決済端末2の公開鍵を暗号化して、端末別公開鍵をカード別公開鍵で暗号化したPCKi（PTkj）を出力する（ステップS7、S7a、S8）。これによって、ICカード1は、電子取引決済端末2の公開鍵を取り出す（ステップS9）。即ち、カード別秘密鍵SCKiで復号化し、端末別公開鍵PTkjを得る（ステップS9a）。

【0036】次に、ICカード1のユニークデータ（固有データ）の出力要求をICカード1に対して与える（ステップS10）。これによって、ICカード1は、ユニークデータXを生成する（ステップS11）。次に、ICカード1のカード別秘密鍵SCKiでユニークデータXを暗号化して（ステップS12、S12a）、暗号化データSCKi（X）を電子取引決済端末2に与える（ステップS13）。次に、電子取引決済端末2は、PCKiで復号化し、ユニークデータXを取り出す（ステップS14、S14a）。

【0037】次に、電子取引決済端末2は、取り出したユニークデータXを、端末別秘密鍵STKjで暗号化して暗号化データSTKj（X）を出力すると共にペリファイ（正しいか否かの確認）指示をICカード1に対して与える（ステップS15、S15a、S16）。これによって、ICカード1は、端末別秘密鍵PTkjで復号化し、ユニークデータXを取り出す（ステップS17、S17a）。

【0038】そして、ICカード1は、ペリファイチェックする（ステップS18）。ICカード1は、ペリファイチェックデータを出力し（ステップS19）、電子取引決済端末2に与える。電子取引決済端末2は、与えられたペリファイチェックデータを確認し（ステップS20）、エラーならばエラー表示する（S20a）。

【0039】次に、図5において、電子取引決済端末2は、任意データYを生成する（ステップS21）。次に、電子取引決済端末2は、この任意データYを、

（1）端末の秘密鍵STKj（Y）、又は（2）ICカード1の公開鍵PCKi（Y）のいずれか一方で暗号化し、いずれか一方を出力し加工指示する（ステップS22、S23）。これに対して、ICカード1は、電子取引決済端末2の任意データYを取り出す（ステップS24）。

【0040】即ち、受け取った任意データYを①電子取引決済端末2の公開鍵PTkjで復号化する、及び②ICカード1秘密鍵SCKiで復号化する、の①②の両方を実行し、2つのデータを生成し（ステップS24a）、（1）の場合の取り出しデータ①Y②？、又は（2）の場合の取り出しデータ①？②Yとする（ステップS24a）。

【0041】このようにして復号化されたデータを、それぞれ（a）①をICカード1の秘密鍵SCKiで暗号

化し出力データSCKi（Y）を電子取引決済端末2に与え、及び（b）②を電子取引決済端末2の公開鍵PTkjで暗号化し出力データPTkj（？）を電子取引決済端末2に与える（ステップS25、S26）。更に、（2）の場合の出力データとして、（a）ICカード1秘密鍵SCKiによる暗号化データSCKi（？）、及び（b）電子取引決済端末2公開鍵PTkjによる暗号化データPTkj（Y）を電子取引決済端末2に与える（ステップS25、S27）。

【0042】電子取引決済端末2は、任意データを取り出し、（a）では、ICカード1の公開鍵PCKjで復号化し、（b）では端末の秘密鍵STKjで復号化する（ステップS28、S28a）。（1）の場合の取り出しデータは、（a）Y、及び（b）？である。（2）の場合の取り出しデータは、（a）？、及び（b）Yである（ステップS28a）。

【0043】次に、データをチェックする（ステップS29）。これは、具体的には、（a）及び（b）がそれぞれ正しいY及び？のペアであるか否かを確認する（ステップS29a）。

【0044】（本発明の実施の形態の効果）以上の本発明の実施の形態によれば、ICカード1に公開鍵と秘密鍵とのペアデータが存在せず、システム鍵が電子取引端末2にのみあり、ICカード1の公開鍵は電子取引決済端末2でのみ取り出すことができる。第1次認証用データを外部より特定できない。第1次認証用データは電子取引端末にのみあり、ICカードのデータより取り出した公開鍵でのみ認証が可能となる。

【0045】また、第1次認証を通過しても、電子取引決済端末2からの任意データから認証確認用データへ加工するためには、公開鍵と秘密鍵とのペアを取得し、ネゴシエーションすることができないため、第2次認証を通過することはできない。従って、第3者が偽造ICカードを自分勝手に公開鍵と秘密鍵のペアを作り出してた場合でも、システム鍵を知らないため、電子取引決済端末2が解読できるSysK（PCKi）を作り出すことができない。このためネゴシエーションの段階で偽造を検知することができる。よって、従来のように電子取引決済端末2がセンタ装置と認証確認しなくても、電子取引決済端末2自身がエラーを検出でき、非常に安全な電子取引決済システムを実現することができる。

【0046】（他の実施の形態）

（1）尚、上述の実施の形態においては、図6に示すように、端末システム用システム鍵SysKを使用した一方向処理71、即ち、端末優位の認証処理を例に構成を説明したが、ICカード優位で認証管理することもできる。この認証管理のための構成を以下に示す。端末優位の認証管理においては、端末システム用システム鍵SysKでICカードの公開鍵ペアの公開鍵（復号化鍵）を暗号化して、ICカード内に自身の公開鍵を持たない。

しかしながら、ICカード優位の認証管理72においては、カードシステム用システム鍵SCdKで、端末の公開鍵ペアの公開鍵（復号化処理）を暗号化し、端末内に自身の公開鍵を持たない。即ち、上述の実施の形態と逆転する立場である。

【0047】(2) また、図6に示すように、端末とICカードの相互認証管理73を実行する方法として、図7に示すように、相互認証用カードを発行し、①端末用システム鍵SysKで認証管理する方法と（図8）、②カードシステム用システム鍵SCdKで認証管理する方法と（図9）において、何れもお互いの自身の公開鍵ペアの公開鍵（復号化鍵）を簡略化して自身の公開鍵を持たない方法を探ることもできる。

【0048】(3) 更に、図6に示すように、独立型相互認証74を実行する方法として、端末もICカードも、公開鍵ペアを2つずつ持ち、互いに上述の①②の仕組みのペアとして、相互に認証チェックする方法を探ることもできる。

【0049】(4) 更にまた、端末システム用システム鍵SysK及びカードシステム用システム鍵SCdKをいつでも変更可能にして運用管理する仕組みを探ることもできる。

【0050】(5) また、システム鍵そのものも、万一漏洩したことが判明したり、又は定期的に変更できる情報処理システムとして、リスクが軽減される。図10は、確認用実データを複数のシステム鍵から復号化してその情報が戻れば該当のシステム鍵が使用されていると判定する情報処理システムの機能構成図である。図10において、ICカード管理用システム鍵81からどの鍵を使用しているかの情報82を確認し、システム鍵(1)83～システム鍵(3)85から確認用実データ86を復号化する。又は、どのシステム鍵を使用しているかの情報を別に持つことも好ましい。

【0051】このような構成の場合の、複数のICカードの認証確認は、図11に示すように、システム鍵(1)の使用に対して、ICカードの有効期間87を設定し、この有効期間に対して延長期間87'も考慮して使用する。システム鍵(2)の使用に対しては、システム鍵(1)の有効期間87の終了に従って有効期間88を設定し、この有効期間88に対しても延長期間88'を考慮して使用する。システム鍵(3)の使用に対しては、システム鍵(2)の有効期間88の終了に従って有効期間89を設定し、この有効期間89に対しても延長期間89'を考慮して使用する。

【0052】(6) 更に、端末システム用システム鍵SysKが解読される場合を仮定し、その対応を示す。すなわち、

(a) ICカード発行時における設定者からの漏洩。この場合、ICカード発行システムそのものが設定情報を元に自動的に生成されるため、設定者自身も実際のシス

テム鍵情報は知りえない。

【0053】(b) ICカード本体から解読。この場合、ICカードの製造時からのICカード別の個別情報（シリアル番号、ユーザ名、ユーザ生年月日など）を土台とした階層構造が形成されるため、その解読から始めねばならない。

10 (c) 万一上述の(a)又は(b)によって解読された場合でも、該当ICカードのみの公開鍵ペアが判明することになるが、ネゴシエーションの一部を捕捉できることになるだけで、ICカードの偽造そのものが成立することはない。従って、容易に第三者がICカードを偽造してシステムに介入し、正当なユーザと同じように電子取引決済することはできない。

【0054】図12は、暗号階層構造の概念図である。図12において、ICカード固有情報90は、各ICカード毎に全て異なる。このICカード固有情報90の階層の下にICカード管理用のシステム鍵91が共通に存在する。この情報はワンショットメモリに書き込まれる。更に、このICカード管理用のシステム鍵91の階層の下に、端末システム用システム鍵SysK92、カードシステム用システム鍵SCdK93、ICカード固有RSAペアの秘密鍵SCki94、その他のICカード内情報95などが存在する。更にまた、端末システム用システム鍵SysK92の階層の下に、ICカード固有のRSAペアの公開鍵PCKiが存在する。

【0055】(7) また、システム鍵SysKを電子取引決済端末側で図13に示す手順で暗号化処理する。すなわち、システム鍵SysKのデータに対して所定の第1暗号化アルゴリズム101を使用して少なくとも1人に割り当たされた第1パスワードデータ102によりランダム化処理して暗号化されたシステム鍵SysKを生成する。

【0056】さらに、特定の管理人などにのみ割り当たされた特定人固有の第2パスワードデータ103により、第1暗号化アルゴリズム101と同じかまたは異なる第2暗号化アルゴリズム104を使用して1回以上のランダム化処理して、第1パスワードデータ102から鍵暗号文を生成し、この鍵暗号文を特定の管理人などにより保管管理する。

40 【0057】(8) また、ICカードを使用する他、磁気カード、磁気バブルメモリ回路などを使用することも好ましく、また、電子取引決済端末は、通信機能を有するパーソナルコンピュータやワークステーションなどが備えるハードウェア構成に、上述の処理を実行するためのソフトウェアを搭載することで実現することができる。

【0058】

【発明の効果】以上述べたように本発明は、カードに、予め、システム鍵で暗号化し生成したカード別ペアの公開鍵と、生成したカード別ペアの秘密鍵と、ユニークデ

ータとを設定しておき、端末に、予め、端末用システム鍵と、端末用公開鍵と、端末用秘密鍵とを設定しておき、上述の認証を実行することで、端末とセンタ装置との間でユーザ確認（認証）するためにオンライン通信する必要がなく、オフラインで端末がカードの偽造を検知でき、システム的な鍵が漏洩してもシステム全体の危機に陥ることがない。

【図面の簡単な説明】

【図1】本発明の実施の形態の電子取引決済システムの構成図である。

【図2】実施の形態の認証シーケンス説明図（その1）である。

【図3】実施の形態の実施の形態の認証シーケンス説明図（その2）である。

【図4】実施の形態のICカードと電子取引決済端末との相互認証の説明図（その1）である。

【図5】実施の形態のICカードと電子取引決済端末との相互認証の説明図（その2）である。

【図6】他の実施の形態のICカード優位の認証管理、電子取引決済端末とICカードとの相互認証管理、独立型相互認証の説明図である。

【図7】他の実施の形態の電子取引決済端末とICカードとで相互認証管理するためのカード発行システムの構成図である。

【図8】電子取引決済端末とICカードとの相互認証管理のうち、電子取引決済端末によるICカードの認証確認の手続きの説明図である。

* 【図9】電子取引決済端末とICカードとの相互認証管理のうち、ICカードによる電子取引決済端末の認証確認の手続きの説明図である。

【図10】実施の形態のICカード管理用システム鍵から確認用実データを得る説明図である。

【図11】実施の形態の複数ICカードの認証確認の説明図である。

【図12】実施の形態の暗号化の階層構造の説明図である。

10 【図13】電子取引決済端末で実行されるシステム鍵SysKの暗号化処理手順の説明図である。

【符号の説明】

1 ICカード

2 電子取引決済端末

3 ICカード発行システム

SH_o 発行機関の秘密鍵

PH_o 発行機関の公開鍵

SysK 端末用システム鍵

SCdK ICカード用システム鍵

SCK_i ICカード別秘密鍵

PCk_i ICカード別公開鍵

STk_j 端末別秘密鍵

PTk_j 端末別公開鍵

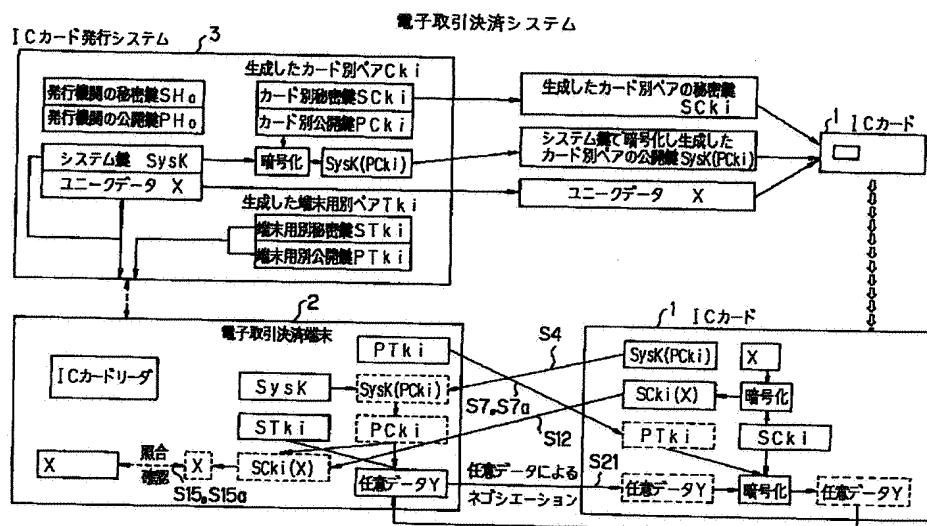
SysK(PTk_i) システム鍵で暗号化されたICカード別公開鍵

X ICカード1内で生成されるユニークデータ

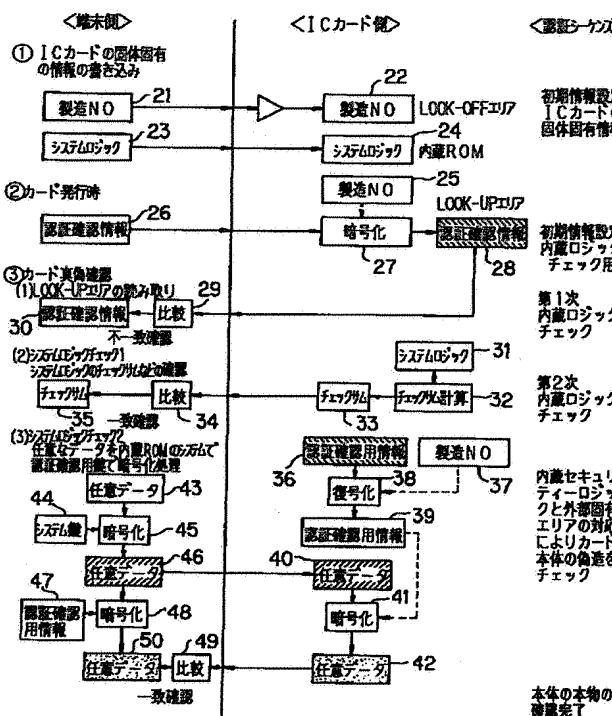
Y 電子取引決済端末2内で生成される任意データ

*

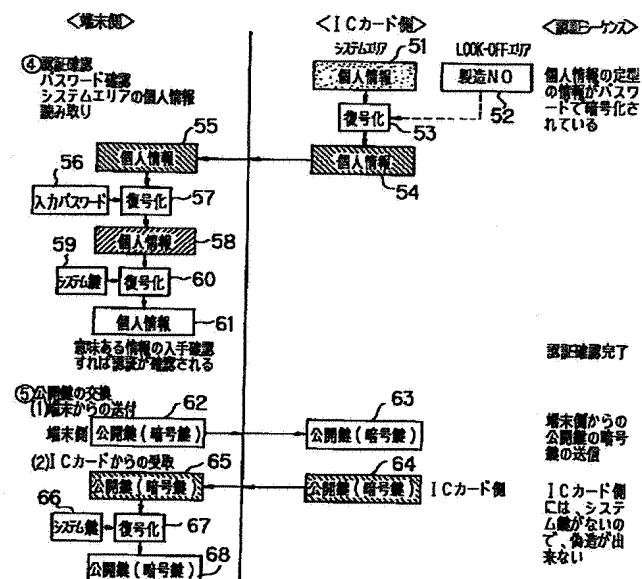
【図1】



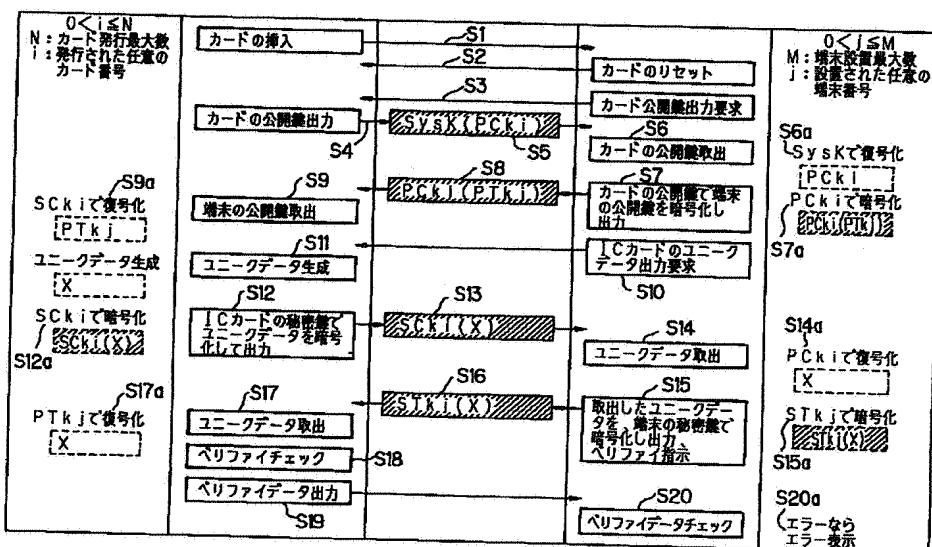
【図2】



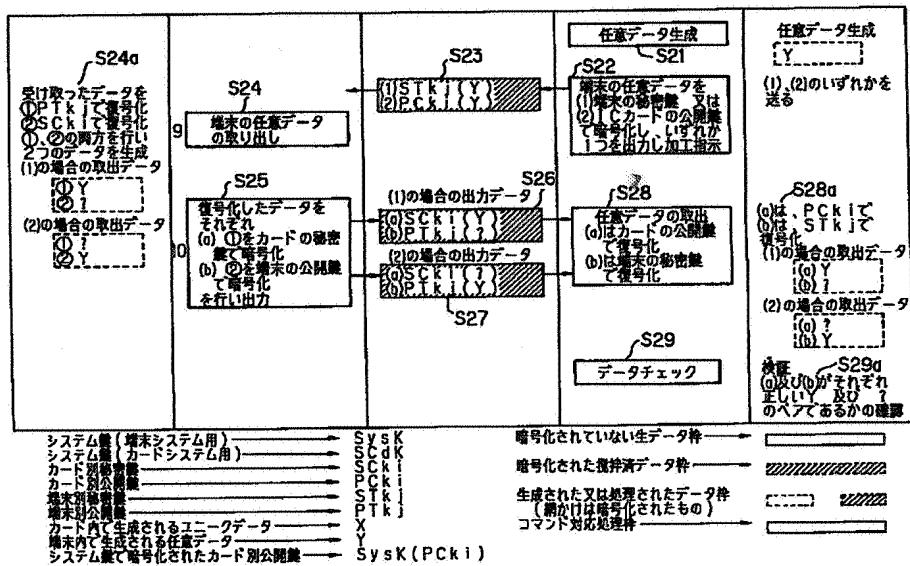
【図3】



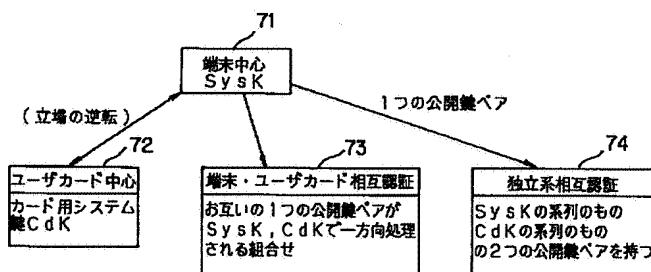
【図4】



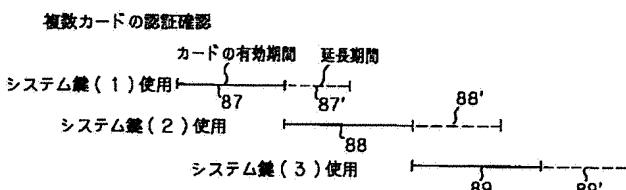
【図5】



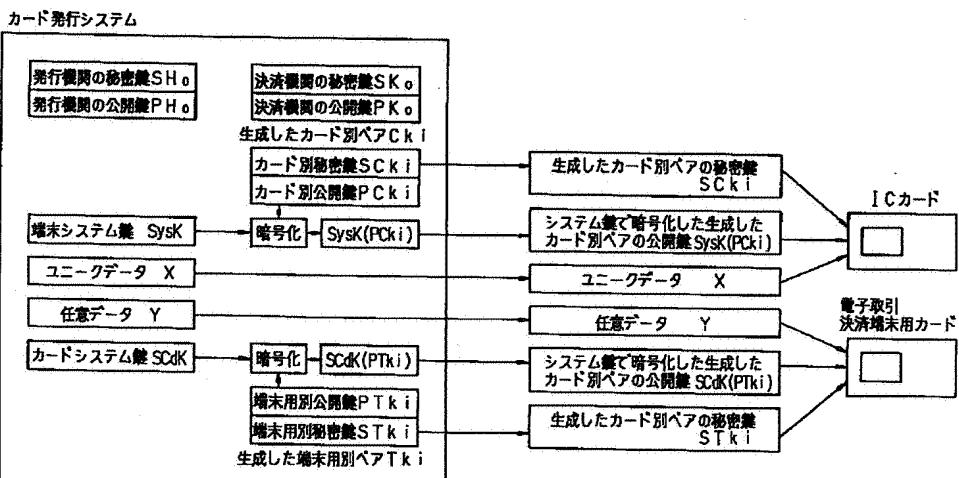
【図6】



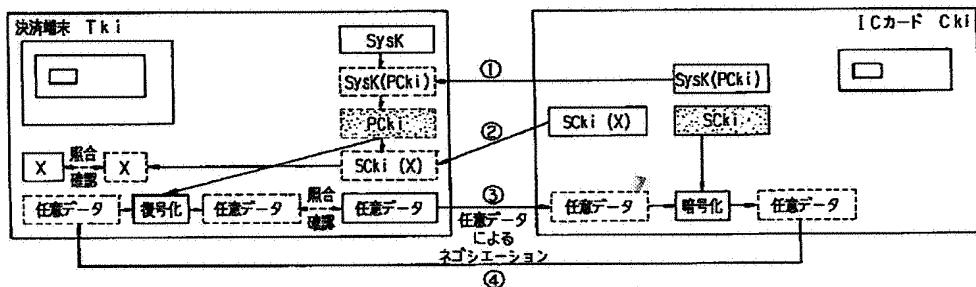
【図11】



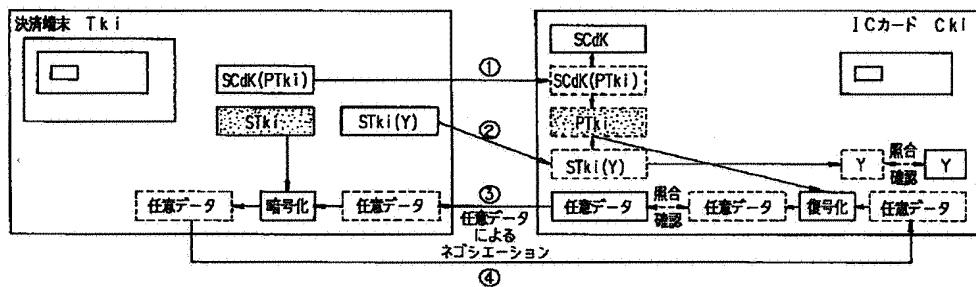
【図7】



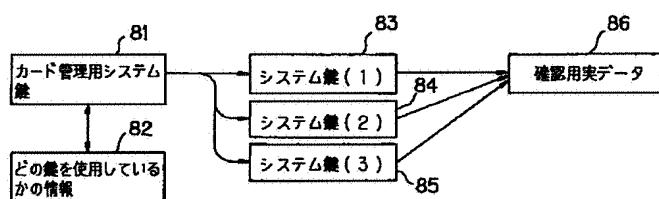
【図8】



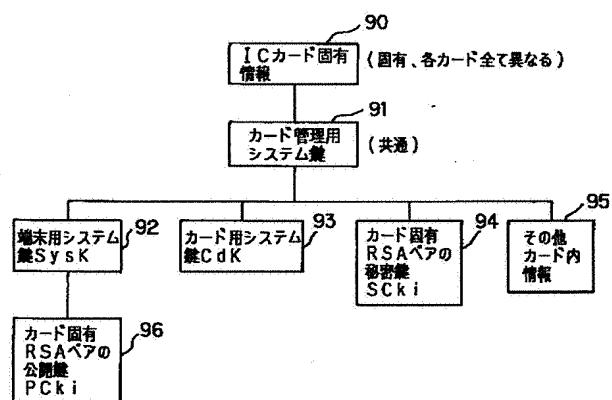
【図9】



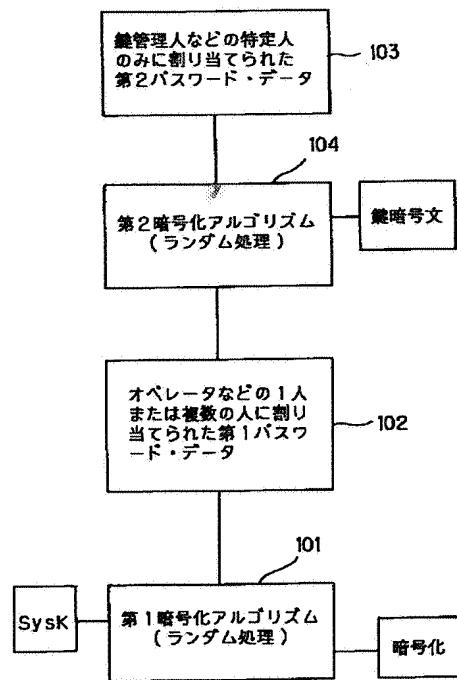
【図10】



【図12】



【図13】



フロントページの続き

(51)Int.Cl.⁶G 06 K 17/00
19/10

識別記号

F I

G 06 F 15/30

3 4 0

G 06 K 19/00

3 5 0 A

R